REMARKS

The non-final Office Action dated August 23, 2010 has been received and reviewed. Claims 1-13, 15-25, and 27-29 are pending in the subject application. Each of claims 1, 6, 8-13, 19-25, and 27-29 is amended herein. Care has been exercised to introduce no new matter. Applicants respectfully request reconsideration of the present Application in view of the above amendments and the following remarks.

Rejections based on 35 U.S.C. § 101

Claim 19 and its dependent claims have been rejected under 35 U.S.C. § 101 as ostensibly being directed to non-statutory subject matter. Applicants have amended claims 19-25 and 27-29 to recite "computer-accessible storage medium" rather than "computer-accessible media" to clarify that media of claimed embodiments of the present invention are limited to non-transitory media. Applicants believe the amended claims overcome the 35 U.S.C. § 101 rejections. As such, Applicants respectfully request withdrawal of the 35 U.S.C. § 101 rejections of claims 19-25 and 27-29.

Rejections based on 35 U.S.C. § 103

A) Applicable Authority

Title 35 U.S.C. § 103(a) declares that a patent shall not issue when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." The Supreme Court in *Graham v. John Deere* counseled that an obviousness determination is made by identifying the scope and content of the prior art, the level of ordinary skill in the prior art, the

differences between the claimed invention and prior art references, and secondary considerations. *Graham v. John Deere Co.*, 383 U.S. 1 (1966).

To support a finding of obviousness, the initial burden is on the Office to establish the clear articulation of the reason(s) why the claimed invention would have been obvious. *See* MPEP § 2142. The analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. *See* MPEP § 2143; *See also KSR v. Teleflex*, 127 S. Ct. 1727 (2007). In determining the differences between the prior art and the claims, the question under 35 U.S.C. 103 is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *See* MPEP § 2141.02(I).

To reach a proper determination of obviousness, the Examiner must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the Examiner must then determine whether the claimed invention "as a whole" would have been obvious at that time to that person. Knowledge of applicant's disclosure must be put aside in reaching this determination. Impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. *See* MPEP § 2142.

B) Rejection of Claims 1, 12, and 19

Claims 1, 12, and 19 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2002/0095591 to Daniell, et al. (hereinafter, "Daniell") in view of U.S. Publication No. 2004/0003279 to Beilinson, et al. (hereinafter, "Beilinson"). As a *prima facie* case of obviousness cannot be established for the rejected claims based upon Daniell in view of Beilinson, Applicants respectfully traverse this rejection, as hereinafter set forth.

Independent Claim 1

Independent claim 1, as amended herein, recites a method for prioritizing user application preferences based on user input data. The method comprises recognizing, at a computing device of a user, user input data relevant to a first application as a prioritized user choice setting associated with the first application, wherein the prioritized user choice setting determines at least one property of execution of at least one event of the first application. The method further comprises securing, at the computing device of the user, the prioritized user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits a second application from modifying the prioritized user choice setting associated with the first application without authorization from the user.

Still further, the method comprises receiving, at the computing device of the user, a request from the second application to modify the prioritized user choice setting associated with the first application and, in response to receiving the request from the second application to modify the prioritized user choice setting associated with the first application, generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application.

The method further comprises receiving, at the computing device of the user, input from the user approving the modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application modifying the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request

received from the second application. The method also comprises modifying, at the computing device of the user, the prioritized user choice setting in accordance with the received user input. Further, the method comprises restoring, at the computing device of the user, the access control indicator to prohibit further modification by the second application of the prioritized user choice setting associated with the first application.

As such, embodiments of the claimed invention are directed towards preventing an application from modifying user settings without receiving user approval of the modifications *prior* to modification. Further, the user interface for receiving approval of modifications from the user is not generated until *after* a request for modifications is received from the second application. As explained in the as-filed application, this is done to prevent applications from automatically reasserting original settings even when the user has expressed changed preferences for prioritized settings, so that a user is not automatically stuck with their initial user preferences indefinitely.

In contrast, Daniell provides methods of reasserting initial security settings to be automatically reset to their authorization settings, in direct conflict with the claimed embodiments of the present invention. In particular, Daniell is significantly distinct from claimed embodiments of the present invention in at least three ways. First, Daniell permits modification of security changes without user approval. *Daniell,* Abstract. In contrast, claim 1 provides a limitation of securing a prioritized user choice setting as a protected value using an access control indicator. In particular, the access control indicator requires authorization from a user prior to a second application modifying the prioritized user choice setting. Contrary to this limitation of claim 1, Daniell provides methods to secure settings by only allowing modifications to occur if a user is listed on an access control list. *Daniell,* ¶ [0004]. As such, Daniell fails to

teach or suggest "securing, at the computing device of the user, the prioritized user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits the second application from modifying the prioritized user choice setting associated with the first application without authorization from the user," as recited in amended independent claim 1. Further, in the invention recited in claim 1, authorization from the user is received at an approval user interface that is generated "in response to receiving the request from the second application to modify the prioritized user choice setting associated with the first application." This is contrary to the disclosure of Daniell.

Secondly, Daniell is distinct from claim 1 in that Daniell "corrects" security changes by "automatically modif[ying] the security settings in order to return the changed settings to their activation state." *Daniell,* Abstract. In contrast, amended independent claim 1 recites "generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application." Since a user authorization is required in response to a request to modify the prioritized user choice setting, the modification is ***not*** automatic and, accordingly, is distinguished from Daniell. As such, it is respectfully submitted that Daniell fails to describe, "in response to receiving the request from the second application to modify the prioritized user choice setting associated with the first application, generating an approval user interface on the computing device of the user, the approval user interface requesting authorization from the user to modify the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application," as recited in amended independent claim 1.

Thirdly, Daniell fails to disclose "receiving, at the computing device of the user, input from the user approving the modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application" prior to making any modifications. Rather, Daniell describes notifying the user *after* the changes have been "restored" to their activation state. See, *Daniell* at Abstract ("The security application then transmits a message to one or more users to alert the user of the detected change in the security settings.") As such, Daniell fails to disclose any aspects of the present invention related to receiving user input ***in response to a request*** to modify a user setting. Accordingly, Daniell fails to describe, "receiving, at the computing device of the user, input from the user approving the modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application," as recited in amended independent claim 1.

While Daniell provides methods of modifying security settings to their initial values, albeit in a manner that is significantly distinct and contrary to embodiments of the present invention, Beilinson provides methods of enabling an administrator to limit computer functions available to a user. *See Beilinson*, Abstract. Additionally, Beilinson provides embodiments where a user may initiate a request for a temporary privileges increase to access computer functions. *See Id.*, ¶ [0023]. In Beilinson, however, a request to increase privileges initiated by a user is a request to *temporarily* increase privileges. As such, under Beilinson, a user does not request to change the user settings described in the remarks of the restrictions component 214 as illustrated in FIG. 2. *See Id.*, ¶ [0060]. Rather, a user may request to be granted an exception as described in the remarks of the exception component 216 of FIG. 2. *See Id.*, ¶ [0062]. As such, Beilinson fails to disclose modification of user choice settings, i.e., settings within the restriction

component 216 of FIG. 2, based on a request received from a user, moreover a second application. Accordingly, Beilinson fails to disclose, "modifying, at the computing device of the user, the access control indicator to permit modification of the prioritized user choice setting associated with the first application to be consistent with the modification request received from the second application," as recited in the rejected claims.

For at least the above-cited reasons, it is respectfully submitted that a *prima facie* case of obviousness for rejected claim 1 cannot be established based upon Daniell in view of Beilinson as these references, alone or in combination, fail to describe each and every limitation as set forth in amended independent claim 1. As such, Applicants respectfully submit that claim 1, as amended, overcomes the 35 U.S.C. § 103(a) rejection thereof. Accordingly, Applicants respectfully request the 35 U.S.C. § 103(a) rejection of claim 1 be withdrawn.

Independent claim 12

Independent claim 12, as amended herein, recites a system for storing user choice settings in a data repository to prevent undesired modifications thereto. The system comprises a registry for storing a user choice setting associated with a first application as a protected value in a registry key, wherein the user choice setting determines at least one property of execution of at least one event of the first application, and wherein the user choice setting comprises at least one of a user preference relating to a file association, an autoplay setting, contents of a start menu, a registered client, a protocol handler, a MIME type handler, a task association, an internet explorer home page, a reset Web page setting, and a sidebar setting. The system further comprises an access control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application and an approval user interface to control modifications to the user choice setting.

The approval user interface is generated on a computing device of the user in response to receiving a request from the first application or another application to modify the user choice setting. Additionally, the approval user interface modifies the ACL to permit writing to change the protected value in the registry key to a modified user choice setting. In particular, the approval user interface modified the ACL upon obtaining approval to modify the user choice setting.

As such, embodiments of the claimed invention are directed towards preventing an application from modifying user settings without receiving user approval of the modifications *prior* to modification. Further, the user interface for receiving approval of modifications from the user is not generated until *after* a request for modifications is received from an application. As explained in the as-filed application, this is done to prevent applications from automatically reasserting original settings even when the user has expressed changed preferences for settings, so that a user is not automatically stuck with their initial user preferences indefinitely.

In contrast, Daniell provides methods of reasserting initial security settings to be automatically reset to their authorization settings, in direct conflict with the claimed embodiments of the present invention. In particular, Daniell is significantly distinct from claimed embodiments of the present invention in at least three ways. First, Daniell permits modification of security changes without user approval. See, *Daniell,* Abstract. In contrast, claim 12 recites securing a user choice setting as a protected value using an access control indicator. In particular, the access control indicator requires authorization from a user prior to an application modifying the user choice setting. Contrary to the invention of claim 12, Daniell describes methods to secure settings by only allowing modifications to occur if a user is listed on an access control list. *Daniell,* [0004]. As such, Daniell fails to teach or suggest "an access

control list (ACL) to secure the registry key, wherein the ACL prevents the first application or another application from modifying the user choice setting associated with the first application," as recited in amended independent claim 12. In particular, in the invention of amended independent claim 12, approval must be obtained through an approval user interface that is generated "in response to receiving a request from the first application or another application to modify the user choice setting."

Secondly, Daniell is distinct from claim 12 in that Daniell "corrects" security changes by "automatically modif[ying] the security settings in order to return the changed settings to their activation state." *Daniell,* Abstract. In contrast, claim 12 provides for generating an approval user interface to receive authorization from a user to modify the user choice setting. Since a user authorization is required in response to a request to modify the user choice setting, the modification is not automatic and, accordingly, is distinguished from Daniell. As such, Daniell fails to desccribe, "upon obtaining approval to modify the user choice setting, [the approval user interface] modifies the ACL to permit writing to change the protected value in the registry key to a modified user choice setting," as recited in amended independent claim 12.

Thirdly, Daniell fails to describe receiving user approval for the modifying of security settings to their activation state. Rather, Daniell describes notifying the user *after* the changes have been "restored" to their activation state. See, *Daniell* at Abstract ("The security application then transmits a message to one or more users to alert the user of the detected change in the security settings.") As such, Daniell fails to describe any aspects of the invention recited in amended independent claim 12 related to receiving user input in response to a request to modify a user setting. Accordingly, Daniell fails to describe, "obtaining approval to modify the user choice setting," as recited in amended independent claim 12.

While Daniell provides methods of modifying security settings to their initial values, albeit in a manner that is significantly distinct and contrary to embodiments of the present invention, Beilinson provides methods of enabling an administrator to limit computer functions available to a user. *See Beilinson*, Abstract. Additionally, Beilinson provides embodiments where a user may initiate a request for a temporary privileges increase to access computer functions. *See Id.*, ¶ [0023]. In Beilinson, however, a request to increase privileges initiated by a user is a request to *temporarily* increase privileges. As such, under Beilinson, a user does not request to change the user settings described in the remarks of the restrictions component 214 as illustrated in FIG. 2. *See Id.*, ¶ [0060]. Rather, a user may request to be granted an exception as described in the remarks of the exception component 216 of FIG. 2. *See Id.*, ¶ [0062]. As such, Beilinson fails to disclose modification of user choice settings, i.e., settings within the restriction component 216 of FIG. 2, based on a request received from a user, moreover from an application. Accordingly, Beilinson fails to disclose, "an approval user interface to control modifications to the user choice setting, wherein the approval user interface is generated on a computing device of the user *in response to receiving a request from the first application or another application to modify the user choice setting*, and wherein the approval user interface, upon obtaining approval to modify the user choice setting, *modifies the ACL to permit writing to change the protected value in the registry key to a modified user choice setting*" as recited in amended claim 12.

For at least the above-cited reasons, it is respectfully submitted that a *prima facie* case of obviousness for rejected claim 12 cannot be established based upon Daniell in view of Beilinson as these references, alone or in combination, fail to describe each and every limitation as set forth in amended independent claim 12. As such, claim 12, as amended, overcomes the 35

U.S.C. § 103(a) rejection thereof. Accordingly, Applicants respectfully request withdrawal of the 35 U.S.C. § 103(a) rejection of claim 12.

Independent claim 19

Independent claim 19 recites a computer-accessible medium having components for performing a method of safely modifying user application preferences for when and how an application is to operate on a computer of a user. The method comprises recognizing user input data relevant to the application as a user choice setting, wherein the user choice setting determines at least one property of execution of at least one event of the application. The method further comprises securing the user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits the application from modifying the user choice setting.

Still further, the method comprises receiving a request from the application to modify the user choice setting. Additionally, in response to the request from the application to modify the user choice setting, an approval user interface requesting authorization from the user to modify the prioritized user choice setting is generated in accordance with the modification request received. The method also comprises receiving input from the user approving modification of the user choice setting associated with the application to be consistent with the request received from the application.

Further, the method comprises modifying the access control indicator to permit modification of the user choice setting associated with the application to be consistent with the modification request received. Additionally, the method comprises modifying the user choice setting in accordance with the received user input. The method also comprises restoring the access control indicator to prohibit further modification of the user choice setting. Further, the

method comprises generating a change notification to the user once the user choice setting has been modified.

As such, independent claim 19 is directed towards preventing an application from modifying prioritized user settings without receiving user approval of the modifications *prior* to modification. Further, the user interface for receiving approval of modifications from the user is not generated until *after* a request for modifications is received from an application. As explained in the as-filed application, this is done to prevent applications from automatically reasserting original settings even when the user has expressed changed preferences for settings, so that a user is not automatically stuck with their initial user preferences indefinitely.

In contrast, Daniell provides methods of reasserting initial security settings to be automatically reset to their authorization settings, in direct conflict with the claimed embodiments of the present invention. In particular, Daniell is significantly distinct from claimed embodiments of the present invention in at least three ways. First, Daniell permits modification of security changes without user approval. See, *Daniell,* Abstract. In contrast, claim 19 recites securing a prioritized user choice setting as a protected value using an access control indicator. In particular, the access control indicator requires authorization from a user prior to an application modifying the prioritized user choice setting. Contrary to this limitation of claim 19, Daniell provides methods to secure settings by only allowing modifications to occur if a user is listed on an access control list. See, *Daniell* at ¶ [0004]. As such, Daniell fails to describe "securing the prioritized user choice setting as a protected value using an access control indicator, wherein the access control indicator prohibits the application from modifying the prioritized user choice setting," as recited in independent claim 19. In particular, prior to modifying a prioritized user choice setting, authorization is received at an approval user interface

that is generated "in response to the request from the application to modify the prioritized user choice setting."

Secondly, Daniell is distinct from claim 19 in that Daniell "corrects" security changes by "automatically modif[ying] the security settings in order to return the changed settings to their activation state." See, *Daniell* at Abstract. In contrast, claim 19 recites "generating an approval user interface requesting authorization from the user to modify the prioritized user choice setting in accordance with the modification request received." Since a user authorization is required ***in response to a request*** to modify the prioritized user choice setting, the modification is not automatic and, accordingly, is distinguished from Daniell. As such, Daniell fails to describe "generating an approval user interface requesting authorization from the user to modify the prioritized user choice setting in accordance with the modification request received," as recited in independent claim 19.

Thirdly, Daniell fails to receive user approval for the modifying of security settings to their activation state. Rather, Daniell notifies the user *after* the changes have been "restored" to their activation state. See, *Daniell* at Abstract ("The security application then transmits a message to one or more users to alert the user of the detected change in the security settings.") As such, Daniell fails to describe any aspects of the invention of claim 19 related to receiving user input in response to a request to modify a prioritized user setting. Accordingly, Daniell fails to describe, "receiving input from the user approving modification of the prioritized user choice setting associated with the application to be consistent with the request received from the application," as recited in independent claim 19.

While Daniell provides methods of modifying security settings to their initial values, albeit in a manner that is significantly distinct and contrary to embodiments of the present

invention, Beilinson provides methods of enabling an administrator to limit computer functions available to a user. *See Beilinson*, Abstract. Additionally, Beilinson provides embodiments where a user may initiate a request for a temporary privileges increase to access computer functions. *See Id.*, ¶ [0023]. In Beilinson, however, a request to increase privileges initiated by a user is a request to *temporarily* increase privileges. As such, under Beilinson, a user does not request to change the user settings described in the remarks of the restrictions component 214 as illustrated in FIG. 2. *See Id.,* ¶ [0060]. Rather, a user may request to be granted an exception as described in the remarks of the exception component 216 of FIG. 2. *See Id.,* ¶ [0062]. As such, Beilinson fails to disclose modification of user choice settings, i.e., settings within the restriction component 216 of FIG. 2, based on a request received from a user, moreover an application. Accordingly, Beilinson fails to disclose, "modifying the access control indicator to permit modification of the prioritized user choice setting associated with the application to match the value stated in the request received from the application," "modifying the prioritized user choice setting to match the value stated in the request received from the application in accordance with the received user input," and "restoring the access control indicator to prohibit further modification of the prioritized user choice setting."

For at least the above-cited reasons, it is respectfully submitted that a *prima facie* case of obviousness for rejected claim 19 cannot be established based upon Daniell in view of Beilinson as these references, alone or in combination, fail to describe each and every limitation as set forth in amended independent claim 19. As such, Applicants respectfully submit that claim 19 overcomes the 35 U.S.C. § 103(a) rejection thereof. Accordingly, Applicants respectfully request the 35 U.S.C. § 103(a) rejection of claim 19 be withdrawn.

C) Rejection of Claims 2-8, 10, 11, 15-18, 20-25, 28, and 29

Claims 2-8, 10, 11, 15-18, 20-25, 28, and 29 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Daniell and Beilinson and in further view of U.S. Publication No. 2002/0143961 to Siegel, et al. (hereinafter "Siegel"). It is respectfully submitted that a *prima facie* case of obviousness of the rejected claims cannot be established based upon Daniell in view of Beilinson, and in further view of Siegel. As such, Applicants respectfully traverse this rejection, as hereinafter set forth.

Each of dependent claims 2-8, 10, 11, 15-18, 20-25, 28, and 29 depends, either directly or indirectly, from one of independent claims 1, 12, and 19 and, accordingly, it is respectfully submitted that these claims are patentable over Daniell in view of Beilinson for at least the above-cited reasons. Further, it is respectfully submitted that Siegel fails to cure the deficiencies set forth above with respect to Daniell in view of Beilinson, nor is Siegel relied upon for teaching such deficiencies. As such, withdrawal of the 35 U.S.C. § 103(a) rejections of these claims is respectfully requested as well. Each of claims 2-8, 10, 11, 15-18, 20-25, 28, and 29 is believed to be in condition for allowance and such favorable action is respectfully requested.

D) Rejection of Claims 9, 13, and 27

Claims 9, 13, and 27 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Daniell and Beilinson, in view of Siegel and in further view of U.S. Patent No. 6,370,141 to Giordano III, et al. (hereinafter "Giordano"). As a *prima facie* case of obviousness cannot be established based upon Daniell in view of Beilinson, in view of Siegel and in further view of Giordano, Applicants respectfully traverse this rejection, as hereinafter set forth.

Each of dependent claims 9, 13, and 27 depends, either directly or indirectly, from one of independent claims 1, 12, and 19 and, accordingly, it is respectfully submitted that these

claims are patentable over Daniell and Beilinson in view of Siegel for at least the above-cited reasons. Further, it is respectfully submitted that Giordano fails to cure the deficiencies set forth above with respect to Daniell and Beilinson in view of Siegel, nor is Giordano relied upon for teaching such deficiencies. As such, withdrawal of the 35 U.S.C. § 103(a) rejections of these claims is respectfully requested as well. Each of claims 9, 13, and 27 is believed to be in condition for allowance and such favorable action is respectfully requested.

CONCLUSION

For at least the reasons stated above, claims 1-13, 15-25, and 27-29 are believed to be in condition for allowance. Applicants respectfully request withdrawal of the pending rejections and allowance of the claims. If any issues remain that would prevent issuance of this application, the Examiner is urged to contact the undersigned – 816-474-6550 or kadsmith@shb.com (such communication via email is herein expressly granted) – to resolve the same.

The fee for a one-month extension of time is submitted herewith by way of electronic payment. It is believed that no additional fee is due. However, if this belief is in error, the Commissioner is hereby authorized to charge any amount required, or credit any overpayment, to Deposit Account No. 19-2112, referencing attorney docket number 304666.01/MFCP.143750.

Respectfully submitted,

/ Kristin D. Smith /

Kristin D. Smith
Reg. No. 63,545

TLB/KSS/jc
SHOOK, HARDY & BACON L.L.P.
2555 Grand Blvd.
Kansas City, MO 64108-2613
816-474-6550